AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Samsung Galaxy cellular telephone, black in color, serial number R28K51H06YH, as described in attachment A

Case No. M-19-1734-M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Southern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Section 554	Knowingly and unlawfully export or attempt to export from the United States, any merchandise, article, or object, to wit: AK-47 Style Firearms, as defined by the United States Munitions List, in violation of 22 USC 2778 and 18 USC 554.

The application is based on these facts:

See Attachment "C"

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Approved by AUSA Andrew Henry
7/24/19

Applicant's signature

Ryan McTaggart, HSI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 7/24/19

Judge's signature

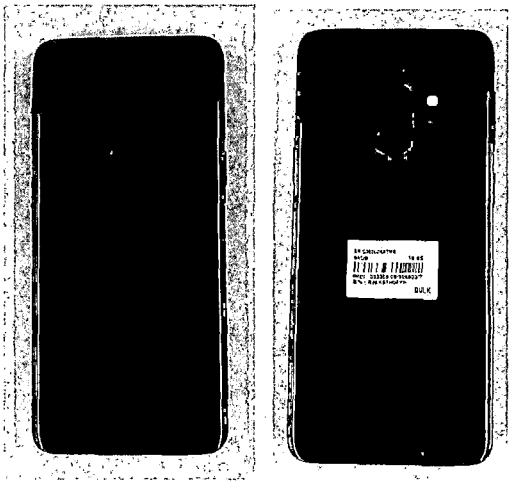
City and state: McAllen, Texas

J. Scott Hacker, United States Magistrate Judge
Printed name and title

ATTACHMENT "A"

Description of property to be searched:

1. One (1) Samsung Galaxy cellular telephone, black in color, serial number R28K51H06YH, and IMEI number 353309/09/306803/7; currently in the possession of Homeland Security Investigations, 5901 South International Parkway, McAllen, Texas



ATTACHMENT "B"

1. All records on the Devices described in Attachment A that relate to violations of firearms and ammunition smuggling including:

a. Any and all text messages, including deleted text messages;

b. Any and all call history logs, including included deleted call history;

c. Any and all emails and instant messages, including deleted emails and instant messages;

d. Any and all photographs and videos, including deleted photographs and videos;

e. Any and all telephone contacts, addresses reflecting names, addresses, telephone numbers, pager numbers, fax numbers, and/or telex numbers;

f. Lists of customers and related identifying information;

g. Types, amounts, and prices of firearms trafficked as well as dates, places, and amounts of specific transactions;

h. Any information related to sources of firearms (including names, addresses, phone numbers, or any other identifying information);

i. Any information recording travel itinerary;

j. All bank records, checks, credit card bills, account information, and other financial records;

k. Any other articles that would constitute a violation of the above offenses.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
MCALLEN DIVISION

IN THE MATTER OF THE SEARCH OF one Samsung Galaxy cellular telephone, black in color, serial number R28K51H06YH, and IMEI number 353309/09/306803/7; (See Attachment A), CURRENTLY LOCATED AT Homeland Security Investigations Office 5901 South International Parkway McAllen, Texas	Case No. M-19-1734-M

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

ATTACHMENT "C"

I, Ryan McTaggart, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to seize and search one (1) Samsung Galaxy cellular telephone, black in color, serial number R28K51H06YH, and IMEI number 353309/09/306803/7 (hereinafter referred to as **TARGET DEVICE**), which is currently stored, in law enforcement's possession, at the Homeland Security Investigations ("HIS") Office, 5901 South International Parkway, McAllen, Texas.

2. I am a Special Agent with Homeland Security Investigations, United States Department of Homeland Security ("DHS"), and currently assigned to the HSI McAllen Office in McAllen, Texas. I have been so employed since June of 2016. Prior to HSI, I was a Border

Patrol Agent and employed with the United States Border Patrol from January 2008 until June 2016. I am a graduate of the Criminal Investigator Training Program ("CITP") and HSI Special Agent Training program ("HSISAT") at the Federal Law Enforcement Training Center in Glynco, Georgia. I am an investigative or law enforcement officer within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516. In connection with my official duties, I investigate violations of Title 8, 18, 19, 21, 22, and 31 of the United States Code and related offenses. These investigative duties include investigation of export control laws which primarily include but are not limited to the Arms Export Control Act (AECA), the Export Administration Regulations (EAR), the International Emergency Economic Powers Act ("IEEPA") and the Trading with the Enemy Act ("TWEA"). I have also received training including but not limited to investigative techniques, export investigations, firearms trafficking investigations, and conspiracy investigations. I have participated in and have conducted investigations which have resulted in the arrests of individuals who have smuggled, received, purchased, and acquired firearms, ammunition, and other defense articles, as well as the seizure of firearms, ammunition, and other defense articles, and the proceeds derived from those criminal activities. In addition, I have conducted follow-up investigations concerning the concealment of firearms, ammunition, and other defense articles, assets, currency, bank records, and the identification of co-conspirators through the use of ledgers, records, telephone bills, photographs, and other documents. As a result of these investigations I have assisted in executing search warrants and collecting and preserving evidence.

3. Based upon my training, experience, and participation in export offense investigations and investigations into the financial implications which result from violations of United States export laws, I know:

a. That firearms traffickers very often use wireless telephones to communicate, negotiate and coordinate illicit transactions with associates in relation to firearms trafficking activities;

b. It is common for individuals involved in trafficking firearms, ammunitions, and defense articles, to use cellular telephones to communicate with other violators to provide instructions, give directions, and or discuss other details regarding the procurement and smuggling of firearms, ammunition, and defense articles;

c. That firearms traffickers very often use wireless telephone capabilities to photograph firearms, ammunition, defense articles, and or currency with the intention of sending photographs as attachments in text messaging or via electronic mail from their wireless telephones in an effort to prove possession of firearms, ammunition, defense articles and/or currency to associates;

d. That firearms traffickers commonly store phone numbers, direct connect numbers, electronic mail address, names and identities of associates in their wireless telephones;

e. That firearms traffickers commonly store photographs, text messages, electronic mail messages and other documents or information in their wireless telephone's memory in relation to violations of United States export laws; and

f. That firearms traffickers commonly carry multiple wireless telephones.

4. This affidavit is intended to show that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

5. The following paragraphs are furnished to established probable cause in support of this warrant:

a. On March 27, 2019, a confidential source ("CS"), who has previously provided reliable information, stated the CS had been contacted by an individual, later identified as Juan HERNANDEZ (hereafter referred to as "HERNANDEZ," regarding the CS attaining and selling firearms to HERNANDEZ. The CS stated HERNANDEZ provided 956-701-5282 as HERNANDEZ contact number.

b. On April 18, 2019, in response to an administrative subpoena, HSI received information from T-Mobile which identified the subscriber for 956-701-5282 as Juan Garcia, at what appears to be a fictitious address. A review of the toll information revealed HERNANDEZ, utilizing telephone number 956-701-5282, was in contact with 956-627-7040 (identified as the telephone number of the **TARGET DEVICE**).

c. On May 1, 2019, SAs received information from a Federal Firearms Licensee regarding the suspected straw purchase of a 5.7 x 28 caliber pistol by Felipe TUDON (hereafter referred to as TUDON).

d. Based upon training and experience, SAs know that a 5.7 x 28 caliber pistol is highly trafficked firearm which, when purchased in close proximity to the United States-Mexico International Boundary, is often intended to be smuggled into Mexico.

e. On May 2, 2019, a source of information ("SOI"), who has previously provided reliable information in the past, stated the SOI had been contacted by HERNANDEZ, from telephone number 956-715-0679, regarding the SOI acquiring firearms for HERNANDEZ. The SOI stated HERNANDEZ was involved in acquiring firearms which were intended to be smuggled into Mexico. The SOI stated HERNANDEZ introduced the SOI to "Mario," later identified as Mario FIERRO, who HERNANDEZ identified as HERNANDEZ's "boss," via telephone, after the SOI stated the SOI did not believe HERNANDEZ was serious about purchasing firearms.

f. The SOI stated after being introduced to FIERRO by HERNANDEZ, the SOI and FIERRO discussed the sale of multiple firearms, which were intended to be smuggled into Mexico, from the SOI to FIERRO.

g. On May 12, 2019, SAs received information from a Federal Firearms Licensee that a .50 caliber rifle was ordered by Francisco SANCHEZ.

h. Based upon training and experience, SAs know that a .50 caliber rifle is highly trafficked firearm which, when purchased in close proximity to the United States-Mexico International Boundary, is often intended to be smuggled into Mexico.

i. On May 15, 2019, SAs interviewed TUDON, and TUDON stated TUDON was recruited by HERNANDEZ to purchase the 5.7 x 28 caliber pistol and HERNANDEZ provided TUDON with the money to purchase the firearm.

j. During a second interview of TUDON, TUDON stated prior to purchasing the 5.7 x 28 caliber pistol, HERNANDEZ and TUDON stopped at Fierro Auto Sales where HERNANDEZ picked up the money used to purchase the firearm.

k. On May 18, 2019, in response to an administrative subpoena, HSI received information from T-Mobile which identified the subscriber for 956-715-0679 as Juan Salinas at what appears to be a fictitious address. A review of the toll information revealed HERNANDEZ, utilizing telephone number 956-715-0679, was in frequent contact with 956-627-7040 (the telephone number for the **TARGET DEVICE**).

l. On May 25, 2019, SAs interviewed SANCHEZ. SANCHEZ stated SANCHEZ left the .50 caliber rifle which SANCHEZ purchased at SANCHEZ friend "Mario's" residence, later identified as Mario FIERRO, and SANCHEZ stated SANCHEZ also purchased a 5.7 x 28 caliber pistol which SANCHEZ left with SANCHEZ friend "Juan Diego." During the interview, SANCHEZ placed multiple telephone calls to "Mario" at 956-627-7096 and "Juan Diego" at 956-678-0665 in order for them to bring the firearms to SANCHEZ' residence to be verified. Later, the .50 caliber rifle and 5.7 x 28 caliber pistol were delivered by Juan LOREDO. ATF SAs issued SANCHEZ a warning letter for straw purchasing. A few days later the .50 caliber rifle and 5.7 x 28 caliber pistol were seized by ATF SAs.

m. On June 13, 2019, an UCA contacted FIERRO, via telephone at 956-627-7096, and FIERRO told the UCA that FIERRO usually purchased new firearms from local stores. The UCA asked FIERRO if FIERRO wanted to meet to purchase the firearms or if FIERRO wanted to have the firearms on the other side and FIERRO stated FIERRO's brother handled "that." The UCA then asked FIERRO about the serial numbers on the firearms and FIERRO stated the UCA did not need to worry and if the UCA wanted the serial numbers on the firearms, said firearm serial number could be removed before the UCA sold the firearms to FIERRO.

n. On July 23, 2019, FIERRO was encountered at the Hidalgo, Texas, Port of Entry, and stated FIERRO's telephone number was 956-627-7040 (the telephone number for the **TARGET DEVICE**). A search of the **TARGET DEVICE** revealed text messages from HERNANDEZ, in May of 2019, using telephone number 956-715-0679, to FIERRO, on the **TARGET DEVICE**, regarding HERNANDEZ having ammunition for the firearms. During the text messages HERNANDEZ refers to the firearms as "Chivos." "Chivos" is a slang term, commonly used by individuals involved in smuggling firearms, ammunition, and other defense articles, to describe AK-47 style firearms.

o. A search of the **TARGET DEVICE**, also revealed, on May 27, 2019, 956-678-0665, a telephone number associated with LOREDO and the delivery of firearms purchased by SANCHEZ, sent text messages to the **TARGET DEVICE** which included photographs of the warning letter which was served to SANCHEZ by ATF SAs on May 25, 2019.

p. In addition, a search of the **TARGET DEVICE**, revealed multiple text messages from 956-358-7884, stored as contact "Juan Crackhead," regarding the sale of multiple firearms from "Juan Crackhead" to FIERRO.

6. The **TARGET DEVICE** is currently in the lawful possession of HSI McAllen, located at 5901 South International Parkway, McAllen, Texas. The **TARGET DEVICE** came into HSI McAllen SA's possession in the following way: On July 23, 2019, FIERRO was encountered at the Hidalgo, Texas, Port of Entry, and the **TARGET DEVICE** was detained to prevent the destruction of, or tampering with, evidence. The **TARGET DEVICE** was secured at the HSI McAllen office for safekeeping. Therefore, I seek this warrant out of an abundance of caution to be certain that a search of the **TARGET DEVICE**, will comply with the Fourth Amendment and other applicable laws.

7. The **TARGET DEVICE** is currently in storage at the HSI McAllen office 5901 South International Parkway, McAllen, Texas. In my training and experience, I know that the **TARGET DEVICE** has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the **TARGET DEVICE** first came into the possession of HSI McAllen special agents.

TECHNICAL TERMS

8. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used primarily for voice communication

through radio signals. These telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a device that records still and moving images digitally. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store any digital data, such as word processing documents, even if the device is not designed to access such files. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive email. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

9. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC DEVICES AND STORAGE

10. As described above and in Attachment B, this application seeks permission to search and seize things that the Devices might contain, in whatever form they are stored. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Even when a user deletes information from a device, it can sometimes be recovered with forensics tools. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

11. Searching for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual

search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment B or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, Homeland Security Investigations intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

METHODOLOGY

12. Following the issuance of this warrant, I will collect and deliver the subject Devices to wireless telephone forensic examiners. These examiners will attempt to power the device, identify whether it is protected by a personal identification number (PIN), determine or circumvent the PIN and retrieve data from the device. Unlike typical computers, many wireless telephones do not have hard drives or hard drive equivalents and store information in volatile memory within the device or in memory cards inserted into the device. Current technology provides some solutions for acquiring some of the data stored in some wireless telephone models using forensic hardware and software. The forensic examiner will determine whether any data associated with this device may be so acquired and, if so, such data will be acquired forensically and the follow-on examination will be conducted using the forensic copy. Even if some of the stored information on the device may be acquired forensically, not all of the data subject to

seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must examine the device manually and record the process and the results using digital photography. This process is time and labor intensive and, depending upon the workload of the few wireless telephone forensic examiners available, may take weeks or longer.

CONCLUSION

13. I submit that this affidavit supports probable cause for a warrant to search the **TARGET DEVICE** and search and seize the items described in Attachment B.

Respectfully submitted,

Ryan McTaggart
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
on 7/24/19, 2019

Hon. J. Scott Hacker
UNITED STATES MAGISTRATE JUDGE